APLIKASI CHIPERTEXT GENERATOR MENGGUNAKAN ALGORITMA VIGENERE BERBASIS MODIFIKASI FIBONACCI

TUGAS AKHIR

Oleh:

REZA PUTRA DEWANGGA
NPM : 0734010232

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
SURABAYA

2012

KATA PENGANTAR

Alhamdulillaahi Robbil 'Alamin.…, Penulis bersyukur kepada Allah SWT atas semua Rahmat, Taufik, dan Hidayah-Nya yang telah diberikan kepada penulis sehingga dapat menyelesaikan Skripsi ini dengan baik.

Dalam menyelesaikan Skripsi ini, penulis berpegang pada teori serta bimbingan dari para dosen pembimbing Skripsi. Dan berbagai pihak yang banyak membantu hingga terselesaikannya Skripsi ini. Skripsi merupakan salah satu syarat bagi mahasiswa untuk menyelesaikan program studi Sarjana Strata Satu (S-1) di Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Pembangunan Nasional "Veteran" Jawa Timur.

Terwujudnya Skripsi ini adalah berkat usaha, kerja keras serta dukungan dari berbagai pihak. Dan tanpa menghilangkan rasa hormat, penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu penulis antara lain:

1. Bapak Prof. Dr. Ir. Teguh Soedarto, MP Selaku Rektor UPN "Veteran" Jawa Timur.
2. Bapak Ir. Sutiyono, MT Selaku Dekan Fakultas Teknologi Industri UPN "Veteran" Jawa Timur.
3. Ibu Dr. Ir. Ni Ketut Sari, MT Selaku Kepala Jurusan Teknik Informatika UPN "Veteran" Jawa Timur.

4. Prof. Dr. Ir. H. Akhmad Fauzi, MMT Selaku pembimbing I yang dengan sabar telah meluangkan banyak waktu, pikiran dan tenaga di antara kesibukan beban-beban kegiatan akademik untuk memberikan bimbingan dan kesempatan penyusun untuk berkreasi dalam proses pembuatan Skripsi ini.
5. Bapak Chrystia Aji Putra, S.Kom selaku pembimbing II yang memberi banyak masukan dan petunjuk khususnya mulai cara memprogram sampai menjadi sebuah aplikasi.
6. Bapak dan Ibu dosen Teknik Informatika yang telah memberikan ilmunya kepada penulis selama kuliah.
7. Ayahanda tercinta, yang merupakan lelaki terhebat yang pernah aku temui dan ibunda tersayang yang juga merupakan perempuan yang kesabarannya tiada bandingnya didunia ini. Adik-adik yang sangat menyayangi aku, terima kasih atas semuanya, aku tidak akan bisa seperti ini tanpa keluargaku. Aku beruntung terlahir dikeluarga ini.
8. Teman-teman seperti Surya(yayak) yang menjadi teman pertama, menjadi *my bound brother*, Abraham yang merupakan teman SMA sampe sekarang dan sebagai guru sepak bola maupun guru catur baik nyata maupun tidak nyata, Bos Yudha yang merupakan teman dari kecil sampe sampai jadi bos ditempat saya bekerja, Lek Agung guru poker yang selalu memberikan chip dan mengajarkan mencari uang dari poker, Dwi dan Erina(Duyung) yang selalu memberi makanan kalau g ada dana, Argo (Jhikey) teman sekaligus guru music dan bahasa inggris

you're the best men, Yoyok(yok's/guru musik legendaris) maaf mas g bisa meneruskan bermusik. Yhonathan (Meta) teman sekaligus vokalis yang hebat semoga bisa masuk 10 besar Indonesia idol tidak hanya 50 besar.

9. Teman-teman kuliah khususnya,,,,,Aris(Brewok) tanpa dirimu q g akan bisa skripsi, kamu telah mengajarkan segala tentang komputer maupun bahasa PHP mulai dari dasar semoga kamu jadi pemilik software house bukan hanya pegawai, Fajar(Bro) "Bersama kita bisa" sungguh kata-kata mutiara yang berarti dalam hidupku, Dzulfikar(Mas Injunk) terima kasih telah memberi dukungan baik moril maupun titip absen, Dimas(Disukai mas-mas) teman pertama dari ospek senasib sependeritaan semoga tetap berteman kita, Tony S.Kom, Satya S.Kom, Novita S.Kom, Misbahlul Munir(Ibet) S.Kom, Dony S.Kom, Wahyu P.(Qyeb) S.Kom, Duwy(Gondrong) S.Kom, Ahmad Nur Setyo Chandra S.Kom, Rizal Febriyanto(Komeng) S.Kom, Anisa(Super Partner) S.Kom Aryo dan Vivi (UPN berdua), Lingga S.Kom. Para anggota TF-E semoga bisa jadi sarjana yang berguna bagi nusa dan bangsa. Teman-teman seperjuangan dalam menyusun skripsi Abet, Endang, Kiky, Panjul, Indra (Bos), Rino (Erno/Pataya) ayo len-jelen. Seluruh teman-teman KKN TM 31 khususnya Achmad Hariyanto(Aha) Derema Berkaber, Dahlia thanks sampai saat ini selalu kamu yang ngeluarin duit, Astria(Trea) S.Kom semoga bisa jadi bupati seperti anda. Anak-anak Kriposoft dengan adanya komunitas ini diInformatika bisa menjadi penolong bagi mahasiswa-mahasiswa untuk saling berbagi ilmu dan meningkatkan ilmu

dibidang indormatika baik formal maupun informal “Lanjutkan”. Dan semua anak TF 2007 dan SI 2007 ayo kita masuk kuliah sama-sama, lulus sama-sama semoga sukses.

10. Teman- teman mahasiswa dan teman-teman diluar kampus yang tak bisa saya sebutkan satu persatu,,,,,terimakasih atas semua dukungan selama ini dan terimakasi atas pertemanannya……

Penulis menyadari bahwa penulisan ini masih jauh dari kesempurnaan, karena tiada gading yang tak retak. Oleh sebab itu, penulis mengharapkan kritik dan saran yang bersifat membangun guna terciptanya kesempurnaan penulisan ini selanjutnya. Semoga penulisan ini dapat menambah wawasan serta ilmu pengetahuan bagi siapa saja yang membacanya.

Surabaya, Mei 2012

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Judul : APLIKASI CHIPERTEXT GENARATOR MENGGUNAKAN ALGORITMA VIGENERE BERBASIS MODIFIKASI FIBONACCI

Pembimbing I : Prof. Dr. Ir. H. Akhmad Fauzi, MMT

Pembimbing II : Chrystia Aji Putra, S.Kom

Penyusun : Reza Putra Dewangga

ABSTRAK

Pada saat ini perkembangan teknologi semakin pesat diberbagai bidang termasuk dibidang informasi. Oleh sebab itu keamanan informasi (*information security*) merupakan hal yang penting dan cara untuk mengamankan pesan yang dikirim tersebut melalui enkripsi. Enkripsi merupakan suatu proses untuk mengubah suatu kata yang bisa dibaca (*plaintext*) menjadi suatu data rahasia yang tidak dapat dibaca (*chipertext*). Tetapi karena semakin berkembangnya zaman maka algoritma-algoritma untuk mengenkripsi data rahasia tersebut ditemukan kelemahan-kelemahan.

Salah satu algoritma yang telah ditemukan kelemahannya oleh Friedrich Kasiski yaitu algoritma *vigenere*. Yang memiliki kelemahan yaitu kata kuncinya masih bisa ditebak dengan metode analisis frekuensi. Dikarenakan algoritma *vigenere* ditemukan kelemahannya, oleh sebab itu maka perlu dilakukan permodifikasian sehingga kelemahan yang ada pada algoritma tersebut tertutupi. Dan cara untuk menutupi kelemahan tersebut dilakukan dengan menambahkan perhitungan *fibonacci*, tetapi karena bilangan *fibonacci* sudah umum diketahui maka rumus *fibonacci* tersebut dilakukan permodifikasian. Dan untuk menerapkannya dibuatlah aplikasi *chipertext* generator menggunakan algoritma *vigenere* berbasis modifikasi *fibonacci*.

Dengan dibuatnya aplikasi *chipertext* generator menggunakan algoritma *vigenere* berbasis modifikasi *fibonacci* maka dapat mengatasi kelemahan yang ada pada algoritma *vigenere* sehingga dapat menjaga kerahasian pesan.

Keyword : keamanan informasi (*information security*), *plaintext, chipertext vigenere, fibonacci*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Dengan melihat perkembangan teknologi dan informasi yang kini semakin pesat di berbagai bidang, maka secara tidak langsung hal tersebut mempengaruhi sistem perdagangan, transaksi dan sistem informasi selama ini. Terutama di era internet ini, semua informasi terkirim suatu jaringan dengan tingkat keamanan yang rendah. Untuk itulah peranan teknologi keamanan informasi benar-benar dibutuhkan. Keamanan Informasi (*Information Security*) merupakan bagian yang sangat penting dari sebuah jaringan komputer terutama yang berhubung dengan internet. Sebuah sistem yang mempermudah dan memanjakan pengguna tidak akan berguna tanpa didukung oleh sistem keamanan yang tinggi. Oleh karena itu, informasi atau data rahasia yang akan dikirim harus disandikan agar tidak dapat dibaca oleh orang lain.

Teknik untuk mengubah informasi yang dapat dibaca/teks asli (*plain text*) menjadi kode-kode tertentu disebut sebagai enkripsi (*encryption*) dan hasilnya disebut *chipertext,* sedangkan teknik untuk mengubah chipertext menjadi plain text disebut deskripsi (decryption). Algoritma yang digunakan untuk proses enkripsi dan deskripsi adalah Algoritma kriptografi (*cryptographic algorithm*) atau sering disebut chiper. Algoritma kriptografi ini bekerja dengan menggunkan kunci (key) seperti kata, nomor maupun frase tertentu. Jika dilakukan enkripsi pada *plaintext* yang sama dengan menggunakan kunci yang berbeda, maka akan menjadi *chipertext* yang berbeda.

Salah satu algoritma dari berbagai macam Algoritma kriptografi (*cryptographic algorithm*) adalah Algoritma *Vigenere Chiper* merupakan salah satu algoritma klasik

yang digunakan untuk menyembunyikan pesan berupa teks dari pihak yang tidak berhak dengan menggunakan teknik substitusi dimana tiap huruf pada plainteks akan disubstitusi menjadi huruf lain berdasarkan kunci yang digunakan. Berbeda dengan *Caesar cipher*, *vigenere cipher* adalah algoritma substitusi jamak dimana suatu huruf plainteks tidak selalu disubstitusi menjadi huruf yang sama, namun disubstitusi berdasarkan kunci yang digunakan.

Kelemahan algoritma *vigenere cipher* muncul jika panjang kunci lebih pendek dari panjang plainteksnya sehingga terdapat perulangan kunci yang digunakan untuk mengenkripsi plainteks tersebut. Kunci yang berulang tersebut menimbulkan celah berupa jumlah pergeseran yang sama untuk setiap plainteks yang disubstitusi oleh huruf pada kunci yang sama sehingga huruf-huruf pesan atau plainteks dapat dikelompokkan berdasarkan kunci yang digunakan. Karena terdapat kelompok huruf-huruf plainteks yang disubstitusi dengan huruf kunci yang sama karena perulangan kunci, maka tiap kelompok huruf-huruf tersebut dapat dikenakan metode analisis frekuensi terhadapnya.

Oleh sebab itu perlu dilakukan modifikasi agar memperkuat kelemahan dari algoritma *vigenere*, salah satu cara untuk memperkuatnya adalah dengan menggunakan modifikasi *Fibonacci* dimana seperti yang kita ketahui *Fibonacci* memiliki deret seperti (0,1,1,2,3,5,8,13,....) dengan adanya *Fibonacci* kita dapat menggunakan kunci yang acak yang panjangnya sama dengan *plaintext* (pendekatan OTP).

1.2. Perumusan Masalah

Permasalahan yang akan dipecahkan dalam kegiatan ini dapat dirumuskan sebagai berikut :

1). Bagaimana meminimalisir perulangan *chipertext* yang dihasilkan?
2). Dibagian mana kita meletakkan rumus *fibonacci* kedalam algoritma *vigenere*?
3). Bagaimana cara memodifikasi rumus *fibonacci* sehingga lebih dinamis?
4). Bagaimana cara agar menghasilkan *chipertext* yang kalimatnya tidak sama ketika diinputkan kata kunci ganjil maupun genap sehingga meminimalisir metode analisis frekuensi?

1.3. Tujuan

Adapun tujuan-tujuan dari dibuatnya penelitian mengenai aplikasi chipertext generator menggunakan algoritma vigenere berbasis modifikasi Fibonacci adalah :

1). Memperbaiki kelemahan pada algoritma vigenere, yang kelemahannya adalah pengulangan kata kunci.
2). Meminimalisir *chipertext* berulang yang dihasilkan oleh algoritma vigenere.
3). Memodifikasi sebuah Algoritma *Vigenere* dengan deretan *Fibonacci* yang sudah di modifikasi.
4). Membangkitkan kata kunci berbasis bilangan *fibonacci* untuk menghilangkan perulangan kata kunci pada sandi *vigenere*
5). Membuat sebuah aplikasi yang dapat melakukan enkripsi dan deskripsi berdasarkan algoritma *Vigenere* yang sudah dimodifikasi dengan *Fibonacci*.

1.4. Batasan Masalah

Di dalam penulisan skripsi ini, agar pembahasan masalah sesuai dengan yang diinginkan dan tidak menyimpang dari apa yang semula dirumuskan, maka penulis menyertakan batasan masalah sebagai berikut :

1). Penelitian ini dilaksanakan pada file berekstensi *.txt.
2). Penelitian dilakukan pada *plaintext* berupa alphabet A hingga Z dan a hingga z, sementara karakter lain dalam ASCII akan diabaikan.
3). Penelitian menggunakan sandi *vigenere*.
4). Penyempurnaan kunci dilakukan dengan menggunakan modifikasi dari deret *fibonacci*.
5). Penelitian menggunakan bahasa pemrograman PHP 5

1.5. Manfaat

Jika aplikasi ini berjalan maka tingkat keamanan dalam mengenkripsi sebuah kata akan semaikin tinggi dan akan sulit dikriptanalisis, baik dengan analisis frekuensi, *known-plaintext attack*, maupun serangan lainnya. Dan juga dapat memperbaiki kelemahan yang ada pada sandi *vigenere*.

1.6. Metodologi Pembuatan Skripsi

Dalam pembuatan Tugas Akhir ini, penulis akan menjelaskan tentang metode yang digunakan selama penulis menyusun dan membuat laporan Tugas Akhir ini.

1). Studi Literatur

Mempelajari konsep atau metode yang akan digunakan sehingga dapat dijadikan panduan untuk merancang aplikasi ini dengan menggunakan PHP 5, serta mencari contoh-contoh apapun untuk membantu penyelesaian Tugas Akhir ini.

2). Survey atau Pengumpulan Data

Setelah mempelajari teori akan dilanjutkan survey ke orang yang berkecimpung dalam masalah jaringan. Disini kita mencari informasi mengenai hal apa saja yang berhubungan dengan keamanan jaringan

3). Perancangan Aplikasi

Pada tahap ini dibuat suatu perancangan aplikasi *Chipertext* generator menggunakan algoritma *vigenere* berbasis modifikasi *fibonacci* .

4). Pembangunan Aplikasi

Pada Tahap ini, aplikasi mulai dibangun sesuai dengan metode yang telah ditentukan dan perancangan yang telah dibuat sebelumnya dengan menggunakan *PHP(Personal Home Page).*

5). Testing dan Evaluasi

Pada tahap ini setelah aplikasi selesai dibuat maka dilakukan pengujian aplikasi untuk mengetahui apakah aplikasi tersebut telah bekerja dengan benar sesuai dengan konsep yang diajukan

6). Penyusunan Buku Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan yang berisi dasar teori, dokumentasi dari hasil perancangan aplikasi *Chipertext* generator menggunakan algoritma *vigenere* berbasis modifikasi *fibonacci* dan hasil yang diperoleh selama mengerjakan tugas akhir. Juga difungsikan sebagai referensi para pembaca dalam mengembangkan Tugas Akhir lebih lanjut.

7). Pembuatan Kesimpulan

Pada tahap ini adalah bagian akhir pembuatan Tugas Akhir yang berisikan kesimpulan dan saran dari hasil pembuatan aplikasi yang diperoleh sesuai dengan dasar teori yang mendukung dalam pengerjaan aplikasi tersebut secara keseluruhan.

1.7. Sistematika Penulisan

Dalam pembuatan tugas akhir ini secara garis besar disusun dalam lima bab, dengan sistematika penulisan sebagai berikut :

BAB 1 : PENDAHULUAN

Bab ini berisi latar belakang masalah, tujuan penulisan, perumusan masalah, batasan masalah, metode penulisan, dan sistematika penulisan.

BAB 2 : TEORI PENUNJANG

Bab ini berisi teori-teori dasar yang digunakan sebagai penunjang dalam pembuatan tugas akhir ini.

BAB 3 : PERANCANGAN DAN PEMBUATAN

Bab ini berisi tentang perancangan perangkat lunak dan mekanik sistem yang akan dibuat.

BAB 4 : PENGUJIAN PROGRAM

Bab ini berisi data-data yang didapat dari pengujian program baik per-blok maupun secara keseluruhan.

BAB 5 : KESIMPULAN DAN SARAN

Bab ini merupakan bab penutup dalam tugas akhir, berisi kesimpulan dan saran dari tugas akhir ini.